



<p>Havells India Limited</p> <p>Havells India Network Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	 HAVELLS
---	---

Havells India

Network Security Management Policy

Version 1.0

Havells India Limited Havells India Network Security Management Policy Version 1.0 Internal	
--	---

Document Control


S. No.	Type of Information	Document Data
1.	Document Title	Havells India Network Security Management Policy
2.	Document Code	HNSMP
3.	Date of Release	20th Feb 2023
4.	Document Superseded	
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head (ISH)	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.0	NA	No change	17th Feb 2023

Havells India Limited Havells India Network Security Management Policy Version 1.0 Internal	 HAVELLS
--	---

Document Scope

This document shall be applicable to the IT Department and the employees/Third Parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution


The Information Security Head (ISH) shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose	5
1.1 Scope	5
1.2 Responsibility	5
1.3 Enforcement	5
1.4 Authority	5
2. Policy	6
2.1 Network Management	6
2.2 Network Access Controls	7
2.3 Network Devices	7
2.4 Backup of network devices	8
2.5 Intrusion Detection and Prevention	9
2.6 Time Synchronization Guidelines	9
2.7 Audit Logging Guidelines	9

<p>Havells India Limited</p> <p>Havells India Network Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
---	---

1. Purpose

Network security, if effectively implemented, will help to minimize information security risk to a great extent and protect Havells against threat of intended/unintended information disclosure. The primary use of Network Security Management Policy is to provide guidance for implementing Network Security controls so as to provide protection against unauthorized access to information/ data/ information assets/network of Havells.

1.1 Scope

This policy shall be applicable to the IT department and the employees/Third Party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Network Security Management Policy.

1.3 Enforcement

All Employees and/or Third Party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

- a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.
- b) Employees and Third Parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head (ISH) approves and enforces this policy and mandates processes to monitor and ensure compliance to this Policy.

2. Policy

2.1 Network Management

Network access controls must be designed to manage and protect information integrity and availability on networks from authorised and unauthorised connections.

2.1.1 Network Diagrams

Network Administrators must maintain a high-level network diagram showing Network connectivity and a logical network diagram showing all network devices. Network diagram must be updated following network changes.

2.1.2 Network Addressing

- a) All networks carrying internal traffic must use private IP addressing;
- b) Tier 1 Internet facing networks or applications can use public IP addressing.

2.1.3 Network Resilience

Network resilience must be provided considering the risk factor in the LAN & WAN using multiple routes and devices to ensure continued operation in the event of a single device or link failure.

2.1.4 Network Hardening

Network systems, including operating systems, equipment and applications must be hardened in accordance to Hardening Document . This must include:


- a) Removing or disabling all unnecessary services;
- b) Removing or disabling all unnecessary (including default) accounts;
- c) Relevant patching applied in a timely and appropriate manner;
- d) Logs are maintained and reviewed where practical;
- e) Backups are maintained where appropriate;
- f) Applying relevant baseline device configuration templates; and
- g) Following best practices and standards where appropriate.

2.1.5 Virtual Local Area Networks (VLANs)

VLANs allow network administrators to automatically limit access to a specified group of users by dividing workstations into different isolated LAN segment. Furthermore, disabling trunking on switches that carry VLANs of differing security zones will also reduce the security risk of data leakage across the VLANs.

- a) VLAN trunking must not be used on switches managing VLANs of differing security zones.
- b) Administrative access should be with respective network lead.
- c) Unused ports on the switches should be disabled wherever applicable

2.1.6 Wireless Networks (WLANs)

<p style="text-align: center;">Havells India Limited Havells India Network Security Management Policy Version 1.0 Internal</p>	
---	---

Wireless networks are inherently insecure. When considering the implementation of security controls for wireless networks the WLAN must be treated in the same manner as for an insecure public access network.


- a) Privately owned wireless devices should not be connected to Havells' DC/DR network without prior business requirement and necessary approvals ;
- b) All APs must be placed to minimize the risk of theft;
- c) Management of the AP through a browser or software must be password protected;
- d) Access to Havells' information asset where a wireless network is involved must use strong authentication and a 'robust' encryption technique;
- e) The SSID identifier for all wireless APs must not identify the device as being part of Havells' network or provide other information about the location of the network.
- f) Default vendor passwords, default cryptographic keys and settings must be changed before use;
- g) All existing patches and fixes to access point and client software must be installed prior to connection, and all subsequently released patches at the earliest opportunity and / or as recommended by OEMs; and
- h) Security features must be used for all wireless implementations, including:
 - i. Mutual Authentication
 - ii. Logging: All accesses must be logged.
 - iii. Encryption

2.2 Network Access Controls

All network access controls must be based on the following principles:

- a) Limit user access on need-to-know basis;
- b) Provide users with the minimum of privileges required for their job;
- c) Require requests for access to a system be authorized by the information owner or designated approving authority;
- d) Access to Havells' wireless network shall be granted to vendors after appropriate business approvals;
- e) For "Guest" network, access shall be granted to users as per business requirement;
- f) For "Vendor or Third party" network, access shall be granted to them for a maximum of 3 months, after appropriate business approvals; and
- g) Users having access to network devices shall be reviewed bi-annually.

2.3 Network Devices

<p style="text-align: center;">Havells India Limited Havells India Network Security Management Policy Version 1.0 Internal</p>	
---	---

- a) Routers, switches, and firewalls shall be configured to provide segregation in the network. This increase both performance and security within the network;
- b) Documented configuration records / backup must be maintained for all critical network devices. SSH service shall be used for logging and executing commands on remote Information Systems wherever applicable;
- c) The following logs should be recorded:
 - i. All administrator level logins to network equipment.
 - ii. All changes to network equipment configuration.

2.3.1 Firewalls

Firewalls are the most commonly used form of gateway device that is used to provide bi-directional communications between network zones.

- a) A stateful firewall shall be used to control access to Havells' network from internet /VPN;
- b) All new system implementations must ensure that traffic generated by Internet facing infrastructure must traverse firewalls before reaching internal infrastructure;
- c) Firewall rules shall be added/removed/modified post required approvals or as per change management process; and
- d) A firewall rule review must be carried out bi-annually.

2.3.2 Routers and Switches


Routers and switches should meet the following configuration guidelines:

- a) The enabled password on the router must be kept in a secure manner;
- b) Disallow the following, wherever applicable:
 - i. IP directed broadcasts;
 - ii. All source routing;
 - iii. All web services running on router;
- c) Use standardized SNMP community strings;
- d) Access rules are to be added as and when business needs arise;
- e) Access to routers shall be based on the employees' role and is linked to active directory; and
- f) The Syslog server should be checked for unauthorized access to the switches.

2.4 Backup of network devices

The following controls shall be implemented for the network assets and services for backup management:

- a) Network assets shall be backed up periodically. The backup for the same shall be available at centralized location;

<p>Havells India Limited</p> <p>Havells India Network Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	
---	---

- b) Adequate backup shall be maintained for the network element configuration and shall be made accessible to authorized personnel only;
- c) Any failure in the backup activity shall be recorded and shall be tracked to closure; and
- d) Also, any failure in the restoration of the backup data for critical network assets shall be recorded and corrective action shall be taken to rectify failure of restoration.

2.5 Intrusion Detection and Prevention


- a) Intrusion detection and prevention technologies (IDS/IPS) must be used to detect and manage unauthorized network accesses;
- b) Network-based IDS/IPS must be used on network segments with internet facing information systems;
- c) Processes must exist to analyses the alerts from an IDS/IPS system and react appropriately to the threat detected;
- d) When deploying IDS/IPS on a network that is not connected to the internet, either directly or indirectly via a cascaded connection, use an IDS that monitors unusual patterns of behaviors or traffic flows, rather than incorporating signatures that detect specific Internet-based communications protocols.

2.6 Time Synchronization Guidelines

- a) Network Administrator should identify Domain controller / authentic NTP which serves as common source, to synchronize the time with a standard time source to Indian Standard Time (IST);
- b) The date / time format should be uniform on the systems, network devices and network security devices.

2.7 Audit Logging Guidelines

- a) General Events to capture such as:
 - i. Network devices/appliances' outage;
 - ii. Successful / unsuccessful login and logout of users;
 - iii. Denial of service events;
 - iv. Configuration accounting for any change on network devices;
 - v. Use of all authorized accounts;
 - vi. Changes to user accounts or privileges (creation, modification, deletion);
 - vii. Excessive login attempts;
- b) Operation events to capture such as:
 - i. Login attempts with failed identification or authentication, also known as failed login attempts;

<p>Havells India Limited</p> <p>Havells India Network Security Management Policy</p> <p>Version 1.0</p> <p>Internal</p>	 <p>HAVELLS</p>
---	---

- ii. Detectable hardware and software errors;
- iii. Log failure and restart events;
- iv. Changes to log files (creation, deletion, and configuration).
- c) Monitoring of network devices availability is performed by NOC team and IT security operations is performed by SOC team
- d) Audit trails shall be archived for 3 months.